UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/532,541	11/17/2005	Daniil Utin	13984-005US1	6860

26161 7590 06/10/2010
FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
06/10/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

Office Action Summary	Application No.	Applicant(s)	
	10/532,541	UTIN, DANIIL	
	Examiner	Art Unit	
	SYED ZIA	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 May 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment and remarks filed on May 24, 2010. The amendments filed on May 24, 2010 have been entered and made of record. Claims are 1-12 are pending for further consideration.

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on May 24, 2010 has been entered.

Response to Arguments

Applicant's arguments filed have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims applicants previously argued that the cited prior arts (CPA) [Challener et al. (U. S. Patent 6,718,468)] does not describe *"generating a first key from a user-supplied unencrypted password," and "encrypting the user-supplied unencrypted password using the first key"*.

This is not found persuasive. The system of cited prior art teaches a associating method in computer system to associate password and secured user public/private key pair, which involves accessing user private key using primary/secondary phase phrases for performing authentication function. After encrypting established user private key with random password, primary/secondary passwords are generated by hashing the primary/secondary pass phrases. The user private key is accessed using primary/secondary phase phrases, for performing authentication function, after performing encryption of random password with the generated primary/secondary passwords, respectively (col. 3 line 55 to col.5 line 24).

As a result, cited prior art does implement and teach a system that relates to generating of password-encrypted key form a user-supplied password and stored in a temporary storage to maintain an access to a secure network communications and access a network (Fig.2a-2b).

Applicants still have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

Therefore, the examiner asserts that cited prior art does teach or suggest the subject matter broadly recited in independent Claims and in subsequent dependent Claims. Accordingly, rejections for claims 1-12 are respectfully maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-12 are rejected under 35 U.S.C. 102(e) as being anticipated by Challener et al. (U. S. Patent 6,718,468).

1. Regarding Claim 1, Challener teach and describe a computer-implemented method for a secure transaction, comprising generating a key from a user-supplied unencrypted password, encrypting the user-supplied unencrypted password using the key, creating a user record, storing the encrypted password in the user record (col.4 line 7 to col.5 line 24)..

2. Regarding Claim 7 Challener teach and describe a computer-executable program residing on a computer, the execution of the program causing the computer to: generate a first key from user-supplied identification data, encrypt the user's identification data using the first key, create a user record and, store the encrypted identification data in the user record (col.4 line 7 to col.5 line 24).

2. Regarding Claim 11 Challener teach and describe a computing device comprising: a memory configured to store a first unencrypted password supplied from a user; and a processor configured to execute instructions to perform a method comprising: generating a first key from the first user-supplied unencrypted password; encrypting the first user-supplied unencrypted password using the first key; storing the encrypted user-supplied password in a user record; upon receiving a login request that includes a second unencrypted password from a would-be user, generating a second key from the second user-supplied unencrypted password in a manner equivalent to generating the first key from the first user-supplied unencrypted password; using the second key to decrypt the first encrypted user-supplied password in the user record; comparing the decrypted password and the second user-supplied unencrypted password to identify a match; upon identifying a match, creating a temporary user session record and storing the second key in the temporary user session record (col.4 line 7 to col.5 line 24).

.

3. Claims 2-6, 8-10 and 12 are rejected applied as above rejecting Claims 1, 7 and 11. Furthermore, Challener teach and describe a system and method of security and user authentication, wherein:

As per Claim 2, further comprising upon user login, generating a key from a would-be user's password using the same algorithm used to generate the key from the originally supplied unencrypted password, retrieving the corresponding user record, decrypting the encrypted

password in the user record using the key, comparing the decrypted password with the would-be user-supplied password to see if they match (col.4 line 7 to line 63).

As per Claim 3, further comprising if the decrypted password and user-supplied password match, creating a temporary session record and storing the key in the session record, otherwise aborting the user login (col.4 line 43 to line 63).

As per Claim 4, further comprising encrypting other sensitive user data using the key and storing the encrypted data in the user record, during a session wherein a session record has been created, using the key stored in the session record to decrypt other encrypted information stored in the user record for use in carrying out some desired action (col. 3 line 55 to col.4 line 7, and col.4 line 66 to col.5 line 24)..

As per Claim 5, further comprising generating a public/private key pair, storing the public key on an application server and the mating private key only another server, encrypting the original user-supplied unencrypted password with the public key and storing the public-key encrypted password on the application server and, fetching the private key from the other server and using it to decrypt selected information on the application server (col.4 line 7 to col.5 line 24)..

As per Claim 6, further wherein the other server is a secure off-site server (col.4 line 7 to line 30).

As per Claim 8, further comprising upon user login, generate a second key from a would-be user's identification data supplied at login using the same algorithm used to generate the first key from the user supplied unencrypted identification data, retrieve the corresponding user record, decrypt the encrypted identification data in the user record using the second key, compare

the decrypted identification data with the would-be user-supplied identification data to see if they match (col.4 line 7 to line 63).

As per Claim 9, further comprising if the decrypted identification data and user-supplied identification data match create a temporary session record and storing the second key in the session record, otherwise aborting the user login (col.4 line 42 to line 63).

As per Claim 10, further comprising encrypt other sensitive user data using the first key and storing the encrypted data in the user record, and during a session wherein a session record has been created, using the second key stored in the session record to decrypt other encrypted information stored in the user record for use in carrying out some desired action (col. 3 line 55 to col.4 line 7, and col.4 line 66 to col.5 line 24).

As per Claim 12, further including: encrypting sensitive user data using the first key; storing the encrypted sensitive user data in the user record; using the second key to decrypt the stored encrypted sensitive user data; and storing the decrypted sensitive user data in the temporary user session record (col. 3 line 55 to col.4 line 7, and col.4 line 66 to col.5 line 24).

.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SYED ZIA whose telephone number is (571)272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
May 27, 2010
/Syed Zia/
Primary Examiner, Art Unit 2431